REMARKS

Claims 1 to 16 remain pending in the above-referenced application and are submitted for the Examiner's reconsideration.

Applicant notes with appreciation the acknowledgment of the claim for foreign priority. Applicant notes the indication that certified copies of the priority documents have not been received. A certified copy of the priority document, *i.e.*, DE 101 10 049.3, is enclosed.

The Examiner objects to the specification because it does not spell out the acronyms EEPROM, CD-ROM, or ASIC. While Applicant does not agree with the merits of this objection, to facilitate matters, the specification has been amended to spell out the acronyms, thereby obviating the present objection. Withdrawal of these objections is therefore respectfully requested.

The Examiner objects to the specification under 37 CFR 1.75(d)(1) for failing to provide proper antecedent basis for the claimed feature that "no byte-wise allocation between input and output data occurs." The specification, e.g., at page 8, lines 20 to 21, provides support for this feature. The sentence is self-explanatory and one skilled in the art would readily understand this feature to mean that an encrypted byte is not the same as a decrypted byte at the same position of the data stream. Accordingly, because the claims are clear and give rise to no ambiguity, and because the specification provides support for the limitations of the claims, no amendment is deemed necessary. Withdrawal of this objection is therefore respectfully requested.

The Examiner objects to the specification under 37 CFR 1.75(d)(1) for failing to provide proper antecedent basis for the feature of "a program code arrangement" of claims 15 and 16. While Applicant does not agree with the merits of this objection, to facilitate matters, claims 15 and 16 have been amended herein without prejudice to obviate the present objection. Withdrawal of these objections is therefore respectfully requested.

Claim 1 stands rejected under 35 U.S.C. § 112, ¶2, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. While Applicant does not agree with the merits of this objection, to facilitate matters, claim 1 has been amended herein without prejudice to obviate the present rejection. Withdrawal of this rejection is therefore respectfully requested.

Claims 11 to 16 stand rejected under 35 U.S.C. § 101 as allegedly including non-statutory subject matter. While Applicant does not agree with the merits of these rejections,

to facilitate matters, claims 11 to 16 have been amended herein without prejudice to obviate the present rejections. Withdrawal of these rejections is therefore respectfully requested.

Claims 1 to 4, and 6 to 16 stand rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of United States Patent No. 5,995,623 to Kawano et al. ("Kawano et al.") and Handbook of Applied Cryptography, by Menezes et al. ("Menezes et al."). Claims 1 to 4, and 6 to 16 are patentable over the combination Kawamo et al. and Menezes et al. for at least the following reasons.

Claim 1 refers to a method of data encryption and provides for encrypting a complete stream of data to be transmitted, wherein no byte-wise allocation between input and output data occurs. The Examiner refers to Kawamo et al. as allegedly disclosing the latter feature, *i.e.*, that no byte-wise allocation between input and output data occurs, and to Menezes et al. as allegedly disclosing the former feature, *i.e.*, encrypting a complete stream of data to be transmitted, and asserts that it would have been obvious to modify the encryption of Kawamo et al. to include the features of Menezes et al. However, it is precisely because the encryption of Kawamo et al. is not performed on a complete data stream that there might not be a byte-wise allocation between the input and output data of Kawamo et al. If the encryption of Kawamo et al. would be modified to include features of Menezes et al. so that an entire data stream is encrypted in an encryption process, then the modified encryption process would result in a byte-wise allocation between the input and output data. That is, an encrypted byte at a particular position of the data stream would correspond to a decrypted byte at the same position of the data stream. Therefore, based on the combination of Kawamo et al. and Menezes et al., one skilled in the art would, at most, recognize two possible and mutually exclusive possibilities for performing encryption, *i.e.*, encrypt *less than the complete data stream* without a byte-wise allocation between input and output data, or otherwise encrypt the complete data stream *with* a byte-wise allocation between input and output data in which there is a true synchronization of the encrypted byte to the decrypted byte that are at the same position. Accordingly, the combination of Kawamo et al. and Menezes et al. does not disclose or suggest the method of claim 1 in which a complete data stream to be transmitted is encrypted and no byte-wise allocation between input and output data occurs. Thus, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 1 or any of its dependent claims, e.g., claims 2 to 4, and 6.

Claim 7 refers to a data encryption system and provides for a data line for transmitting encrypted data that is an encryption of a complete stream of data, where no byte-wise allocation between input and output occurs. As set forth above in support of the patentability

of claim 1, the combination of Kawamo et al. and Menezes et al. does not disclose or suggest these features. Thus, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 7 or any of its dependent claims, *i.e.*, claims 8 to 10.

As further regards claim 7, the claim has been amended herein without prejudice to recite that the encryption of a byte includes a rotation of bits of the byte about a number of positions, where the number depends on an entire history of the encryption of the complete stream of data. Support for the amendment to claim 7 may be found in the specification, e.g., at page 7, lines 1 to 4. Neither Kawamo et al. nor Menezes et al., alone or in combination, disclose or suggest this feature. For this additional reason, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 7 or any of its dependent claims, *i.e.*, claims 8 to 10.

Claim 11 refers to a computer program product having program code which, when executed, cause a computing unit to perform a method, and provides for performing an encryption of a complete stream of data, where no byte-wise allocation between input and output data occurs. As set forth above in support of the patentability of claim 1, the combination of Kawamo et al. and Menezes et al. does not disclose or suggest these features. Thus, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 11 or its dependent claim, *i.e.*, claim 12.

Claim 13 refers to a computer program product having program code which, when executed, cause a computing unit to perform a method, and provides for performing a decryption of a complete stream of data, where no byte-wise allocation between input and output data occurs. As set forth above in support of the patentability of claim 1, the combination of Kawamo et al. and Menezes et al. does not disclose or suggest these features. Thus, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 13 or its dependent claim, *i.e.*, claim 14.

Claim 15 refers to a computer-readable medium, and provides for a program code for performing an encryption of a complete stream of data, where no byte-wise allocation between input and output data occurs. As set forth above in support of the patentability of claim 1, the combination of Kawamo et al. and Menezes et al. does not disclose or suggest these features. Thus, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 15.

Claim 16 refers to a computer-readable medium, and provides for a program code for performing a decryption of a complete stream of data, where no byte-wise allocation between input and output data occurs. As set forth above in support of the patentability of claim 1, the

combination of Kawamo et al. and Menezes et al. does not disclose or suggest these features. Thus, the combination of Kawamo et al. and Menezes et al. does not render unpatentable claim 16.

In view of all of the foregoing, withdrawal of the rejections of claims 1 to 4, and 6 to 16 is requested.

Claim 5 stands rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of Kawano et al., Menezes et al., and United States Patent No. 6,215,875 to Nohda ("Nohda"). Claim 5 is patentable over the combination of Kawano et al., Menezes et al., and Nohda for at least the following reasons.

Claim 5 depends from claim 1 and therefore includes all of the features recited in claim 1. Since Nohda does not cure the deficiencies noted above in support of the patentability of claim 1 over the combination of Kawamo et al. and Menezes et al., it is therefore respectfully submitted that the combination of Kawamo et al., Menezes et al., and Nohda does not render unpatentable this dependent claim for the same reasons set forth above in support of the patentability of claim 1. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988) (any dependent claim that depends from a non-obvious independent claim is non-obvious).

It is therefore respectfully requested that the objections and rejections be withdrawn, and that the present application issue as early as possible.

Respectfully submitted,

KENYON & KENYON LLP

By: [illegible] (Reg. No. 44,777)

Dated: 6/22/06 By _____

Gerard A. Messina
(Reg. No. 35,952)

One Broadway
New York, NY 10004
(212) 425-7200